



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:  
29.12.1997 Bulletin 1997/52

(51) Int. Cl.<sup>6</sup>: **H04L 29/06**

(21) Application number: **97109792.8**

(22) Date of filing: **16.06.1997**

(84) Designated Contracting States:  
**AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL  
PT SE**

(30) Priority: **19.06.1996 US 667524**

(71) Applicant: **AT&T Corp.**  
**New York, NY 10013-2412 (US)**

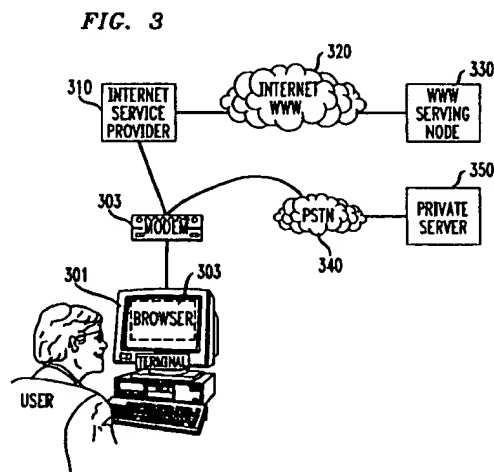
(72) Inventors:  
• **Harwood, Jonathan P.**  
**Morganville, N.J. 07751 (US)**

• **Kimmeth, Thomas**  
**Gladstone, N.J. 07977 (US)**  
• **Nusbaum, Kurt**  
**Downers Grove, Illinois 60515 (US)**

(74) Representative:  
**KUHNEN, WACKER & PARTNER**  
**Alois-Steinecker-Strasse 22**  
**85354 Freising (DE)**

(54) **System and method for automated network reconfiguration**

(57) A method is disclosed for providing an enhanced level of security for sensitive or proprietary information associated with information transactions in a public network, such as the Internet. In carrying out that method, an on-line information transaction is bifurcated between a generalized information access portion of such a transaction and an exchange of sensitive user information. With such a bifurcation, the generalized information access portion of the transaction, which generally would constitute the more substantial (in terms of network resources) portion of the transaction, would be handled via a non-secure network, usually a public network such as the Internet. The portion of the transaction involving sensitive user information, on the other hand, would be handled by a separate secure connection, such as a private network, or intranetwork. An important characteristic of this bifurcation arrangement is the provision of a means for automated reconfiguration of a user terminal as between accessing the Ageneralized information via the non-secure network and access to the secure communications network for the exchange of sensitive user information. Such an automated reconfiguration will be carried out without the necessity for any action on the part of the user, and indeed will be largely invisible to the user.



**Description****FIELD OF THE INVENTION**

5 This invention is related to the field of data communications, and more particularly to a method and means for establishing an automatic reconfiguration of a user terminal among alternative tasks.

**BACKGROUND OF THE INVENTION**

10 With the increasing popularity of personal computers over the last several years has come a striking growth in transaction-oriented computer-to-computer communications (as opposed to bulk-data transfers among such computers). For convenience herein such transaction-oriented computer-to-computer communications will be described by the shorthand term "information transaction". That growth in the use of computers for such information transactions has unquestionably been fueled by the existence of an international infrastructure for implementing such data communications, known as the Internet. And, driven by the burgeoning demand for such information transaction services, the Internet has itself experienced explosive growth in the amount of traffic handled.

At least partly in response to that demand, a new level of accessibility to various information sources has recently been introduced to the Internet, known as the World Wide Web ("WWW"). The WWW allows a user to access a universe of information which combines text, audio, graphics and animation within a hypermedia document. Links are contained within a WWW document which allow simple and rapid access to related documents. Using a system known as the HyperText Markup Language ("HTML"), pages of information in the WWW contain pointers to other pages, those pointers typically being a key word (commonly known as a hyperlink word). When a user selects one of those key words, a hyperlink is created to another information layer (which may be in the same, or a different information server), where typically additional detail related to that key word will be found.

25 In order to facilitate implementation of the WWW on the Internet, new software tools have been developed for user terminals, usually known as Web Browsers, which provide a user with a graphical user interface means for accessing information on the Web, and navigating among information layers therein. A commonly used such Web Browser is that provided by Netscape.

The substantial growth in the use of computer networks, and particularly the WWW, for such information transactions, has predictably led to significant commercialization of this communications medium. For example, with the WWW, a user is not only able to access numerous information sources, some public and some commercial, but is also able to access "catalogs" of merchandise, where individual items from such a catalog can be identified and ordered, and is able to carry out a number of banking and other financial transactions. As will be obvious, such commercial transactions will typically involve sensitive and proprietary information, such as credit card numbers and financial information of a user.

35 Thus, with the growth of commercial activity in the Internet, has also come a heightened concern with security. It is well known that there are persons with a high level of skill in the computer arts, commonly known as "hackers", who have both the ability and the will to intercept communications via the Internet. Such persons are thereby able to gain unauthorized access to various sensitive user information, potentially compromising or misappropriating such information.

40 The vulnerability of such sensitive user information to misuse when so transmitted via the Internet is a phenomena which has only recently received wide public attention. Unless such security concerns can be quickly addressed and alleviated, the commercial development of this new communications medium may be slowed or even stalled altogether.

**SUMMARY OF THE INVENTION**

45 Accordingly, it is an object of the invention to provide an acceptable level of security for sensitive or proprietary information associated with information transactions in a public network, such as the Internet. That object is realized through an arrangement whereby an on-line information transaction is bifurcated between a generalized information access portion of such a transaction and an exchange of sensitive user information. With such a bifurcation, the generalized information access portion of the transaction, which generally would constitute the more substantial (in terms of network resources) portion of the transaction would be handled via a non-secure network, usually a public network such as the Internet. The portion of the transaction involving sensitive user information, on the other hand, would be handled by a separate secure connection, such as a private network, or intranetwork. An important characteristic of this bifurcation arrangement is the provision of a means for automated reconfiguration of a user terminal as between accessing the generalized information via the non-secure network and access to the secure communications network for the exchange of sensitive user information. Such an automated reconfiguration will be carried out without the necessity for any action on the part of the user, and indeed will be largely invisible to the user. In a further embodiment of the invention, a transfer of data is provided from a public to a private network, wherein data selected by a user from a public net-

work site may be arranged and displayed at a user terminal and, subject to further user selection/confirmation activity, thereafter transferred to a private network.

## BRIEF DESCRIPTION OF THE DRAWINGS

5

Figure 1 depicts an illustrative case of information transactions carried out via a public network such as the Internet.

Figure 2 shows the architecture of a browser as would typically be applied for accessing a hypermedia web page.

Figure 3 illustrates the primary elements of the reconfigurable dual-path method of the invention.

Figure 4 depicts in flow chart form the basic jump capability of the methodology of the invention.

10 Figures 5A & 5B (generally designated collectively herein as "Figure 5") depict in flow chart form the "shopping cart" capability of the methodology of the invention.

Figure 6A & 6B (generally designated collectively herein as "Figure 6") depict in flow chart form the stored configuration capability of the methodology of the invention.

15 Figure 7A & 7B (generally designated collectively herein as "Figure 7") depict in flow chart form the off-line form capability of the methodology of the invention.

## DETAILED DESCRIPTION

20 For clarity of explanation, the illustrative embodiment of the present invention is presented as comprising individual functional blocks. The functions these blocks represent may be provided through the use of either shared or dedicated hardware, including, but not limited to, hardware capable of executing software.

Figure 1 depicts an illustrative case of information transactions carried out via the Internet. As seen in the figure, an exemplary user obtains access to the Internet by first connecting, via a Terminal 110 having an associated Browser 111, to an Internet Service Provider 112 selected by the user. That connection between the user and the Internet Service Provider will typically be made via the Public Switched Telephone Network (PSTN) from a modem associated with the user's Terminal to a network node in the Internet maintained by the selected Internet Service Provider.

25 Once the user has obtained access to the selected Internet Service Provider, an address is provided for connection to another user or other termination site and such a connection is made via the Internet to that destination location. As can be seen from the figure, communication via the Internet may be either user-to-user, as from Terminal 110 to Terminal 130, or from a user to a node representing an information source accessed via the Internet, such as Public Site 120.

30 It will of course be understood that the Internet provides service to a large number of users and includes a large number of such Public Sites, but the illustration provides the essential idea of the communication paths established for such Internet communication. It will also be understood that a number of service classifications are supported by the Internet, with the World Wide Web service, which represents a preferred embodiment for the public network aspect of the method of the invention, being one of the currently most heavily trafficked of such services.

35 The Web Browser, such as depicted at 111, can be seen as a software application operating in conjunction with a user terminal (such as Terminal 110) which provides an interface between such a user terminal and the particular functionality of the WWW information site. The architecture of such a browser is generally described in terms of three main components, as illustrated in Figure 2. At the top level is the Browser 201, which enables the acquisition of information pages from a WWW server (beginning, in all cases, with the "home page" for that server), for display at a display device associated with the terminal. The Browser also provides the necessary interface for the terminal with the HTML functionality used by the server to provide access to other linked information layers.

40 The second level of the browser architecture is the TCP/IP Stack 202, which handles the communications protocols used for connecting the terminal to the WWW server. The bottom level of this architecture is the Dialer 203, which typically handles the function of providing dialing and setup digits to a modem, as illustrated at 204, such a modem generally being a part of the terminal. Normally, upon receiving dialing and other setup information from the dialer, the modem would cause a connection to be made via the PSTN to the Internet Service Provider selected for that terminal.

45 After a connection is established in this manner to the Internet Service Provider, an address would be provided for the WWW information node sought to be contacted, a connection to that node made through the Internet, and the home page for that node caused to be displayed at the terminal's display device. A user would then select a key word in that home page, typically by clicking on the word with a mouse or similar device, and, upon transmission of that selection signal to the WWW server, a hyperlink would be created to the linked information layer and the open page of that layer would be caused to be displayed at the user terminal.

50 As explained above, serious questions have been raised in respect to the security of communications via the public Internet. (Note, that the discussion herein is focused on the Internet, and particularly the WWW functionality of the Internet, as a preferred embodiment of such public data communication networks generally, but the methodology of the invention will be applicable to any such network.) To address this problem, the methodology of the invention begins with a bifurcation of the information transaction between a user and the selected information transaction provider into a por-

tion related to sensitive or proprietary user information, and other information comprising that transaction. With such a bifurcation, it becomes possible to provide substantial security for that proprietary information by use of an alternative communications path for that separated portion of the transaction via a private network, or intranetwork -- *i.e.*, a connection between a user's terminal and a secure serving node on that private network. It is anticipated that a coordination means will be established in respect to the management of information among the public and private network elements of the bifurcated information transaction.

In its basic form, this methodology may be carried out by the user terminal initiating a call via the Internet to a selected WWW node, and upon establishing connection to that node, proceeding with the desired information transaction up to the point where an exchange of sensitive or proprietary information were required. At that point the user terminal would be instructed by the WWW server to terminate that connection (*i.e.*, hangup) and to place a new call to an identified private network server for the necessary exchange of sensitive information.

However, in order to accomplish such a dual-path transaction, it is necessary that the browser at the user terminal be reconfigured to provide the dialing, authorization (*i.e.*, login and password), and other needed information for accessing the alternative private network, in order to implement the proprietary portion of the transaction. It will also usually be the case that, upon completion of that private-network transaction, the original dialer, stack and browser configurations will need to be restored, in order for the terminal to retain its normal Internet access functionality. Such a reconfiguration and subsequent restoral of the necessary parameters in the browser, stack and dialer is likely to be well beyond the capabilities of the average user.

Accordingly, as a further embodiment of the inventive methodology, an automated browser reconfiguration means is provided which interoperates with the browser. This browser reconfiguration means is described in detail hereafter and will be referred to as the "Bridging Software".

Figure 3 provides an illustration of the primary elements of the reconfigurable dual-path method of the invention. As seen in the figure, a first path comparable to the Internet link shown in Figure 1, between User Terminal 301 and WWW Serving Node 330 (via Browser 302, Modem 303, Internet Service Provider 310, and Internet 320) is provided. However, an alternative path is now provided from the output of Modem 303 to Private Server 350. That path is illustrated as being via the PSTN, which is generally regarded as being highly secure, but an alternative dedicated or other more-secure path between the User Terminal 301 and the Private Server 350 could as well be provided. In keeping with the discussion above, Browser 302 shown in Figure 3 would also include the Bridging Software installed as a helper application for implementing the automatic reconfiguration of the Browser.

In the operation of this system, a user would normally make an initial connection to an Internet application, such as the application represented by WWW Serving Node 330, which, *e.g.*, might be a shopping application, a financial transaction, or the provision of an enrollment form for off-line preparation. After conducting all, or some portion of an information transaction short of an exchange of sensitive or proprietary information, including a capture by the user's terminal of needed information from the public site, a user provides a signal indicative of an end to that portion of that transaction. During the course of the public portion of the information transaction, specially configured files are sent from the WWW serving node to the Bridging Software associated with Browser 302. Such files contain instructions for the Bridging Software to store information-like products -- *e.g.*, for selected items from a catalog, forms for enrollment, or non-secure portions of a financial transaction, and reconfiguration information for dialing and logging into the private portion of the transaction. The Bridging Software then hangs up the Internet connection, edits the user terminal's browser, stack and dialer files to reconfigure the terminal to connect to the private server. Prior to automatic redialing of the new private site for the user, the Bridging Software may be instructed by the application operating at WWW Server Node 330 to display items chosen for purchase, or to display a form for the end-user to complete off-line before dialing the private application. Upon connecting to the private application and completing the transaction as to the user sensitive information in a private environment, the Bridging Software then restores the end-user software to the dialing and authorization parameters required to dial to the public Internet.

A particularly advantageous application of the automated reconfiguration and information transfer methodology of the Bridging Software is that it adds value to certain WWW servers which do not possess the Common Gateway Interface ("CGI") capability -- *i.e.*, a provision of specialized functions on the server beyond just displaying HTML files, and are accordingly unable to accomplish any transactional processing in respect to items selected by a user. In effect, such a non-CGI server, on its own, can only serve as a "billboard" for the items represented in its database.

However, with the collection and redelivery process of the Bridging Software, a data capture and processing mechanism can be implemented for servers operating in a non-CGI environment -- such servers being incapable of more than the simple delivery of static data packets corresponding to available items. The data set enabled by the Bridging Software is a mechanism for augmenting such limited server capabilities by defining a flexible mechanism for the receipt, display, and delivery of arbitrary data from one site to another.

In such a scenario, the Bridging Software receives a "shopping cart" item list from the host as a data-set defined with a static MIME data packet associated with the Bridging Software. This information comprising the data-set may be updated, displayed to the user in a "read-only" fashion, or presented to the user for order selection.

During the process of interacting with the WWW server, a user may trigger HTML links resulting in additional MIME packets for the Bridging Software being delivered to the client. These packets allow items to be added and/or removed from the specified data set or presented to the user for local confirmation. The user will interact with a pop-up screen provided by the Bridging Software which presents the items available with product information, such as part number, description, unit cost, etc. The user identifies those items which are to be placed into the "shopping cart" and the quantity of items desired. Upon completion of the form, the Bridging Software stores the order in a format suitable for subsequent delivery to the private server site.

An additional feature provided by the methodology of the Bridging Software is an automated mechanism for providing compatibility with user terminals not previously having the Bridging Software included with the terminal's browser. To that end, the Bridging Software located at an accessed public network site initially checks to see if the browser counterpart for that software is loaded at the calling user terminal. If yes, the heretofore described processes of the Bridging Software go forward. If not however, a request is sent through the public host to download the Bridging Software to the calling terminal. After such a download, a helper application loads the Bridging Software to the terminal's browser.

## I. Illustrative Embodiments

A variety of browser reconfiguration applications are supported by the automated browser reconfiguration means of the invention. Four essentially diverse capabilities of this invention, which support such applications, are described hereafter as illustrative embodiments of the invention.

### A. Basic Jump Capabilities

In this configuration, which is illustrated in flow chart form in Figure 4, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (Step 401 of Figure 4). After conducting an information transaction with the selected WWW serving node for some interval (determined in relation to the specific application accessed), the user clicks on a hyper-text link, or picture, to begin an automated process which will cause that public session to be terminated and a new connection established to an alternate private data network (Step 402).

In response to that user action, a data message containing parameter reconfiguration instructions is passed from the WWW server application to the Bridging Software at the user's terminal (Step 403). Upon receiving such instructions, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (Step 404). This reconfiguration is fully automatic and transparent to the user, and includes parameters such as modem dial number, login, password, and TCP/IP addresses. At that point, the Bridging Software causes the modem to disconnect the current data network connection, shutting down the browser, and to then dial the alternate private data network (Step 405).

With the establishment of a connection to the private server on the alternate data network, the user interacts with the alternate data network application as appropriate (Step 406), and after an interval completes his activity with the alternate data network and provides an indication of such completion (Step 407). A data message containing parameter reconfiguration instructions is then passed from the alternate data network application to the Bridging Software (Step 408).

At that point, the Bridging Software again edits the user's on-line communications software parameters, reconfiguring them to dial the original public data network, or another preselected network (Step 409). As with the first reconfiguration, this configuration is automatic and includes parameters such as modem dial number, login, password, and TCP/IP addresses. The Bridging Software automatically causes the current private data network to be disconnected by the modem (Step 410), and if appropriate, causes the original public data network to be redialed (Step 411). When such a reconnection to the public data network is established, the end-user would then continue his application in the public data network.

### B. "Shopping Cart" Capability

With this configuration, illustrated in flow chart form in Figure 5, a user begins by establishing a connection to a WWW application (assuming for the moment that the application is non-CGI enabled) at a serving node for that application, using the Internet browser and modem associated with the user's terminal (Step 501 of Figure 5). Upon finding an item in that application to be saved, or remembered for later consideration, or purchase, the user clicks on a hyper-text link, or picture, representing that item (Step 502). That application then sends a data message to the Bridging Software containing information about the items selected (Step 503) and such information is stored by the Bridging Software.

ware in the "shopping cart" file in the user's terminal (Step 504). Such selection download and storage steps (*i.e.*, steps 502, 503 & 504) are repeated for as many items as the user chooses to select. At any point after the Bridging Software has received the first set of item selection information, the user can instruct the Bridging Software to cause those selected items about which such information has been received to be displayed locally (at the user's terminal), where the user may review or edit (including deletion if desired) the collection of items theretofore selected. The application may also control display characteristics such as color and font for such locally displayed items. Note that in the case of a CGI-enabled application, the application itself will keep track of the items selected by the user and only download the totality of the selected items at the end of the selection process, and accordingly, the described local display option will not be applicable to such a CGI-enabled application.

At the point of completion of his "shopping", the user clicks on a hyper-text link or picture to "check out" (Step 505), which will begin a process of causing a jump to an alternate data network for the completion of sensitive portions of the transaction. To that end, a data message containing parameter reconfiguration instructions is passed from the WWW application to the Bridging Software (Step 506). It is to be noted that, as a security measure, information such as the new dial number, IP address, home page, configuration data (*e.g.*, login, password, DNS address) may be passed over the public network in encrypted form.

Upon receiving such reconfiguration instructions, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (Step 507). This reconfiguration is fully automatic and transparent to the user, and includes parameters such as modem dial number, login, password, and TCP/IP addresses. At that point, the Bridging Software causes the modem to disconnect the current data network connection, shutting down the browser, and to then dial the alternate data network (Step 508).

The Bridging Software passes the stored "shopping cart" data captured from the WWW application to the alternate network application (Step 509), where that data may be displayed for the user, permitting the user to confirm and/or modify the data (Step 510). The user interacts with the alternate data network application as appropriate, and after an interval completes his activity with the alternate data network (Step 511) and thus, by providing an appropriate completion signal to the application, completing the private portion of the information transaction (Step 512). A data message containing parameter reconfiguration instructions is then passed from the alternate data network application to the Bridging Software (Step 513).

The Bridging Software, at this point, again edits the user's on-line communications software parameters, reconfiguring them to dial the original (or another pre-defined) data network (Step 514). As with the first reconfiguration, this configuration is automatic and includes parameters such as modem dial number, login, password, and TCP/IP addresses. The Bridging Software automatically causes the current private data network to be disconnected by the modem (Step 515), and if appropriate, causes the original public data network to be redialed (Step 516). When such a reconnection is established to the point in the public data network where the user had left off to handle the secured aspects of his information transaction, the user would then continue his application in the public data network.

### C. Stored Configuration Capabilities

For this configuration, depicted in flow chart form in Figure 6, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (Step 601 of Figure 6). The user selects a hypertext link or picture associated with the WWW application by clicking on such link or picture (Step 602). A data message containing parameter reconfiguration instructions and an application icon (related to the selected hypertext link or picture) is passed from the WWW application to the Bridging Software (Step 603).

The Bridging Software creates an icon for display at the user's terminal, and saves a Bridging Software configuration file that is associated with that icon (Step 604). Such Bridging Software actions are automatic and multiple selections may be captured in this manner. At this point the user may continue the on-line session, or, if all desired selections have been made, a signal is provided from the user that the session should be discontinued (Step 605). The Bridging Software then automatically disconnects the current data network connection (Step 606).

After disconnecting from the WWW application, and following an interval determined by the user, a new application is selected by the user by clicking on the appropriate new icon displayed at the user's terminal (Step 607). The Bridging Software receives the reconfiguration instructions from the file associated with the selected icon (Step 608).

The Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (Step 609). The Bridging Software then automatically starts the user's Internet browser software and causes the alternate network application to be dialed by the modem associated with that terminal (Step 610). Upon establishing a connection to the alternate network, the user interacts with that application and completes the transaction to the user's satisfaction (Step 611). After a signal is sent to the alternate network indicating such completion of the user's activity (Step 612), a data message containing parameter reconfiguration instructions is passed from the alternate data network application to the Bridging Software (Step 613). That Software then causes the user's

terminal configuration parameters to be reset (Step 614) and the alternate data network to be automatically disconnected (Step 615).

#### D. Off-Line Form Capability

5

In this configuration, depicted in flow chart form in Figure 7, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (Step 701 of Figure 7). The user selects a hypertext link or picture associated with an off-line form application -- an exemplary such form being an HTML-based form -- by clicking on such link or picture (Step 702). A data message containing parameter reconfiguration instructions for the Bridging Software, the selected off-line-form application, and an optional icon (related to the selected hypertext link or picture) is passed from the WWW application to the Bridging Software (Step 703). Note that the selected off-line form may be for either single or multiple use.

10

In the case of a delayed or multiple use of the selected form, the Bridging Software may create an icon for display at the user's terminal, and will save a Bridging Software configuration file that is associated with that icon (Step 704). The form in question is also saved on the user's terminal. Such Bridging Software actions are automatic. At this point the user may continue the on-line session, or, if all desired selections have been made, a signal is provided from the user that the session should be discontinued (Step 705). The Bridging Software then automatically disconnects the current data network connection (Step 706).

15

After disconnecting from the WWW application, two cases are to be considered as to the further processing of the selected form: (1) an immediate single use of the form and (2) either a delayed or multiple use of the form. In the first case, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network. The Bridging Software then automatically starts the user's Internet browser software which is caused to display the off-line form. The user then completes the off-line form and chooses a "Submit Form" button displayed at his terminal.

20

In the second case, the Bridging Software will have created an icon for display at the user's terminal and saved a Bridging Software configuration file associated with that icon. Following an interval determined by the user, the off-line-form application is started by the user by clicking on the new form icon displayed at the user's terminal (Step 707). The Bridging Software receives the reconfiguration instructions from the file associated with the selected icon (Step 708).

25

The Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (Step 709). The Bridging Software then automatically starts the user's Internet browser software which is caused to display the off-line form (Step 710). The user then completes the off-line form and chooses a "Submit Form" button displayed at his terminal (Step 711).

30

In either the first or second case, following activation of the "Submit Form" button, the alternate network application is then caused to be dialed by the Bridging Software. Upon establishing a connection to the alternate network, the form data is passed to the alternate network (Step 712). The user then interacts with that application and completes the application (Step 713). After a signal is sent to the alternate network indicating such completion of the user's activity (Step 714), a data message containing parameter reconfiguration instructions is passed from the alternate data network application to the Bridging Software (Step 715). That Software then causes the user's terminal configuration parameters to be reset (Step 716) and the alternate data network to be automatically disconnected (Step 717).

35

40

#### CONCLUSION

A system and method has been described for the automatic switching of an information transaction between two or more alternate networks. This functionality, which incorporates a reconfiguration means designated herein as the Bridging Software, supports the movement of application specific data from one on-line environment to another. Among potential applications of this process for passing data between different environments are: selected items for purchase ("shopping cart"), captured data from forms, and other server captured data such as web pages visited.

45

The Bridging Software reconfiguration means is intended to work with various Web Browser software implementations, including the Netscape Personal Edition (NPE) Software for Windows 3.1 and 3.11, and which represents a working embodiment for the invention. The Bridging Software installs itself as a helper application within the browser application and utilizes a special MIME type configuration file to pass reconfiguration and "shopping cart" information from the server to the client software.

50

When an application requires a user to re-connect to a private application, a reconfiguration file is passed to the Bridging Software helper application via a CGI script or simple hyper-text link. The helper application disconnects the current data connection, reconfigures the dial parameters (dial #, login password, DNS address, and home page) and initiates the dial program so the end-user can access the private application.

55

When the end-user connects to the private application, the Bridging Software reconfiguration means provides the new "private server" application with data collected from the "public server", and the application resumes in a private,

secure environment.

The Bridging Software allows both short term and long term storage of dial configurations. Configurations passed to the Bridging Software can be designated as single use configurations and discarded after the application has terminated, or saved and displayed to the end-user as a dial choice by the Bridging Software.

Although the present embodiment of the invention has been described in detail, it should be understood that various changes, alterations and substitutions can be made therein without departing from the spirit and scope of the invention as defined by the appended claims. In particular, it is noted that, while the invention has been primarily described in terms of a preferred embodiment based on an automatic reconfiguration between a public and a private data network, any the methodology of the invention will be equally applicable to any set of alternate networks.

## Claims

1. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;  
 receiving information from said serving node in said first data network for effecting a reconfiguration of said communications path for said transaction from said first connection in said first data network to a second connection in a second data network; and  
 automatically connecting said terminal device to a serving node in said second data network via said second connection.

2. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;  
 selecting at least one information item from a data base of said information items provided at said serving node in said first data network;  
 causing said selected information items to be downloaded to said terminal device via said first connection;  
 receiving information from said serving node in said first data network for effecting a reconfiguration of said communications path for said transaction from said first connection in said first data network to a second connection in a second data network; and  
 automatically connecting said terminal device to a serving node in said second data network via said second connection.

3. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;  
 identifying at least one data network application from a data base of said data network applications provided at said serving node in said first data network;  
 receiving information from said serving node in said first data network for reconfiguring said terminal device for implementation of a communication path via an alternate connection between said terminal device and at least one of said identified data network applications in a second data network; and  
 in response to a selection signal from a user, automatically connecting said terminal device to a selected one of said identified data network applications via said alternate connection.

4. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;  
 selecting an off-line form application from a data base provided at said serving node in said first data network;  
 receiving information from said serving node in said first data network for reconfiguring said terminal device for implementation of a communication path via a second connection between said terminal device and said



selected off-line form application in a second data network; and  
in response to, a selection signal from a user, automatically connecting said terminal device to said selected off-line form application.

- 5 5. The method for managing a transaction of Claim 1 or 2 including the further step of recognizing a signal to reconfigure said communications path from said first connection to said second connection.
6. The method for managing a transaction of Claim 3 wherein said selected data network application is operated at a serving node in said second data network.
- 10 7. The method for managing a transaction of Claim 4 wherein said selected off-line form application is operated at a serving node in said second data network.
8. The method for managing a transaction of one of the Claims 1, 2, 6 or 7 wherein said serving nodes in said first and said second data networks are manifested in a common node.
- 15 9. The method for managing a transaction of Claim 1 or 2 wherein said step of receiving information includes the further step of effecting said reconfiguration of said communications path.
- 20 10. The method for managing a transaction of Claim 1 or 2 wherein said step of automatically connecting includes the step of automatically disconnecting said first connection prior to implementation of said second connection.
11. The method for managing a transaction of Claim 1 or 2 including the further steps of:  
25 automatically disconnecting said second connection in response to a user signal; and  
reconfiguring said terminal device to enable, in response to user instruction, an implementation of a connection via an identified data network.
- 30 12. The method for managing a transaction of Claim 11 wherein said step of automatically reconfiguring said terminal device includes the step of effecting said implementation of said connection via said identified data network.
13. The method for managing a transaction of Claim 2 wherein said step of causing said selected information items to be downloaded includes the further step of causing said selected information items to be displayed at said terminal device.
- 35 14. The method for managing a transaction of Claim 13 wherein said displayed selected items can be edited by a user at said terminal device.
15. The method for managing a transaction of Claim 13 wherein display characteristics for said displayed selected items can be controlled at said terminal device.
- 40 16. The method for managing a transaction of Claim 2 wherein said step of automatically connecting includes the step of uploading said selected information items from said terminal device to said service provider via said second connection.
- 45 17. The method for managing a transaction of Claim 3 including the further steps of:  
automatically disconnecting said alternate connection in response to a user signal; and  
reconfiguring said terminal device to enable implementation of a pre-selected connection between said terminal device and an identified data network.
- 50 18. The method for managing a transaction of Claim 17 wherein said step of automatically reconfiguring said terminal device includes the further step of effecting said implementation of said pre-selected connection.
- 55 19. The method for managing a transaction of Claim 4 including the further step of downloading from said serving node in said first data network to said terminal device of an off-line form related to said off-line form application.
20. The method for managing a transaction of Claim 4 including the further step of uploading said downloaded off-line

form from said terminal device to said selected off-line form application, after processing by a user.

21. The method for managing a transaction of Claim 4 including the further steps of:

- 5 automatically disconnecting said connection to said selected off-line form application in response to a user signal; and  
reconfiguring said terminal device to enable implementation of a pre-selected connection between said terminal device and an identified data network.

10 22. The method for managing a transaction of Claim 21 wherein said step of automatically reconfiguring said terminal device includes the further step of effecting said implementation of said pre-selected connection.

23. A method for managing connections between a terminal device and at least one information source/processor wherein at least two of said connections are implemented via separate communications networks, comprising the steps of:

- 15 recognizing a signal for connection to an information source/processor via a communications network other than a communications network for which a predetermined connection is configured;  
causing said terminal device to implement a connection to said information source/processor via said other communications network; and  
20 upon termination of said information source/processor connection via said other communications network, automatically reconfiguring a connection criteria in said terminal device to enable said terminal device to implement, in response to user instruction, a connection via an alternative one of said communications networks.

25 24. The method for managing connections of Claim 23 wherein said recognizing step occurs at a point when said terminal device is connected to a given source/processor.

25. The method for managing connections of Claim 23 wherein information items may be selected by a user at said terminal device from said given source/processor, and including the further step of causing said selected information items to be downloaded from said source/processor to said terminal device.

26. The method for managing connections of Claim 25 wherein said step of effecting connection includes the further step of uploading said selected information items from said terminal device to said other information source/processor.

35 27. The method for managing connections of Claim 26 wherein said selected information items are processed by said user at said terminal device prior to uploading to said other information source/processor.

28. The method for managing connections of Claim 24 including the further step of causing said given source/processor to download to said terminal device configuration data for enabling said step of effecting connection to said other information source/processor.

29. The method for managing connections of Claim 24 including the further step of causing said other source/processor to download to said terminal device configuration data for enabling said step of automatically restoring a prior connection criteria in said terminal device.

30. A method for enhancing security of certain data in an on-line information transaction comprising the steps of:

- 50 bifurcating said information transaction into a first portion comprising said certain data and a remaining portion, wherein said remaining portion is carried out via a public on-line communications connection between a terminal device and a public information server;  
causing said first portion to be carried out via a secure private on-line communications connection between said terminal device and a private information server; and  
automatically reconfiguring network access means in said terminal device to switch between said public connection and said private connection.

FIG. 1

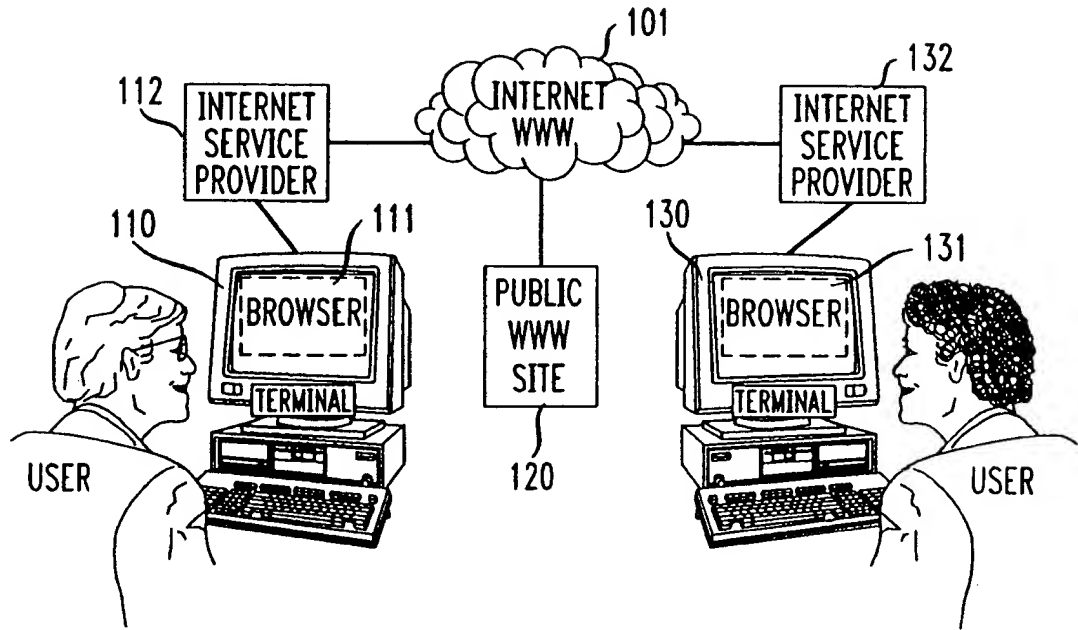


FIG. 2

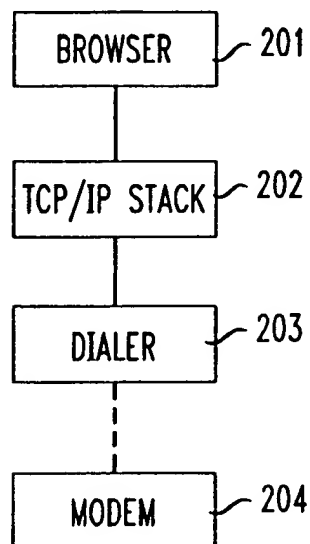


FIG. 3

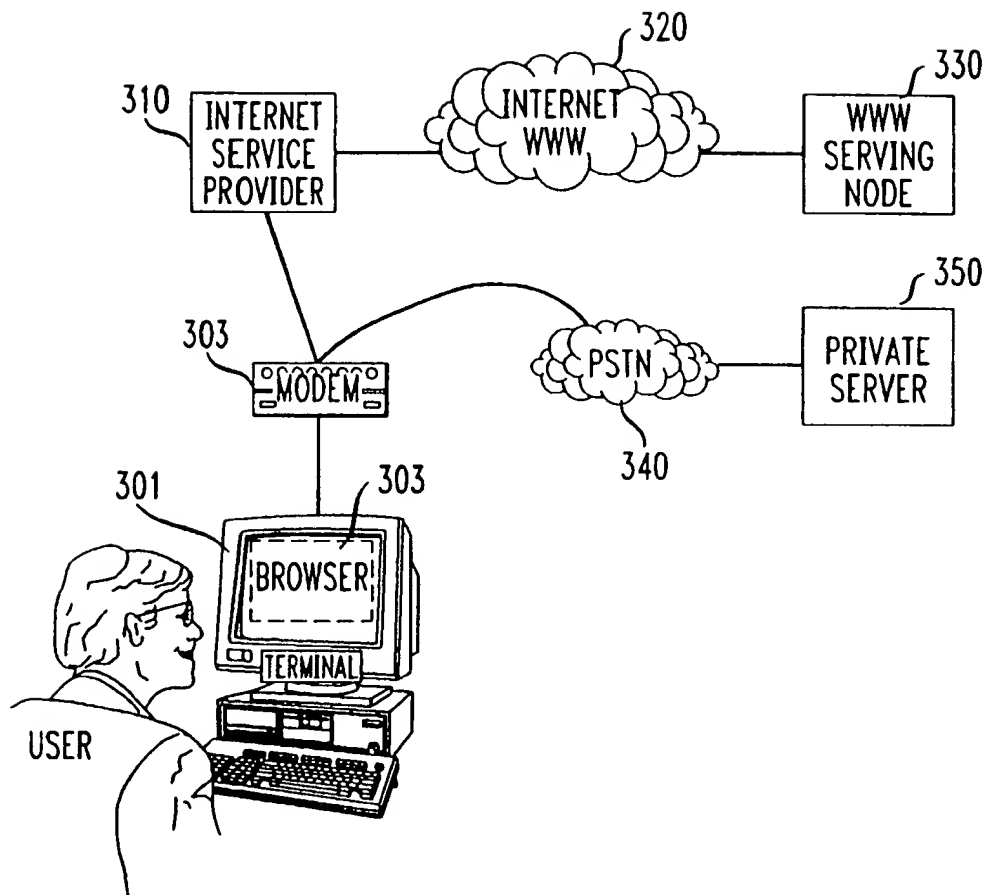


FIG. 4

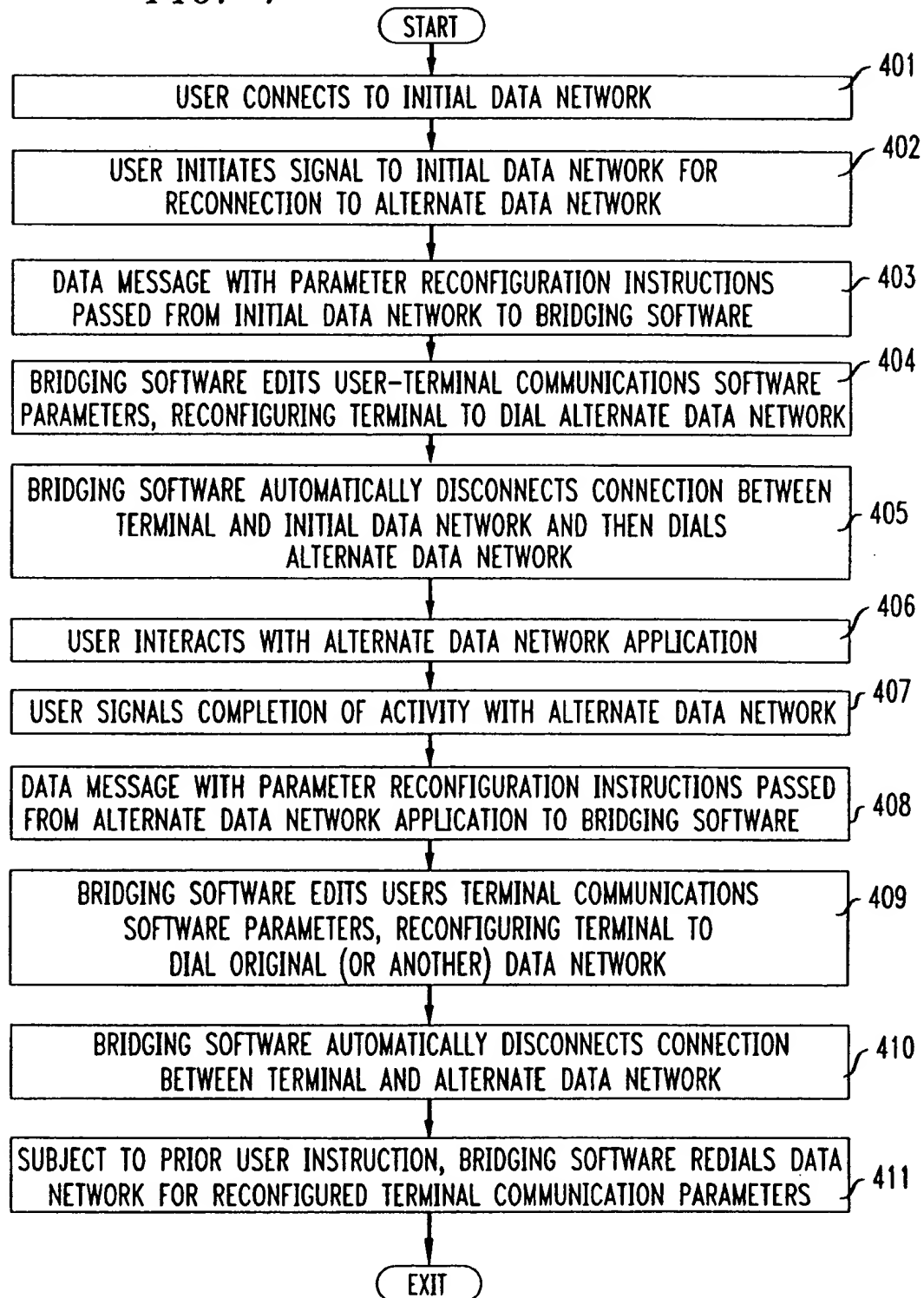


FIG. 5A

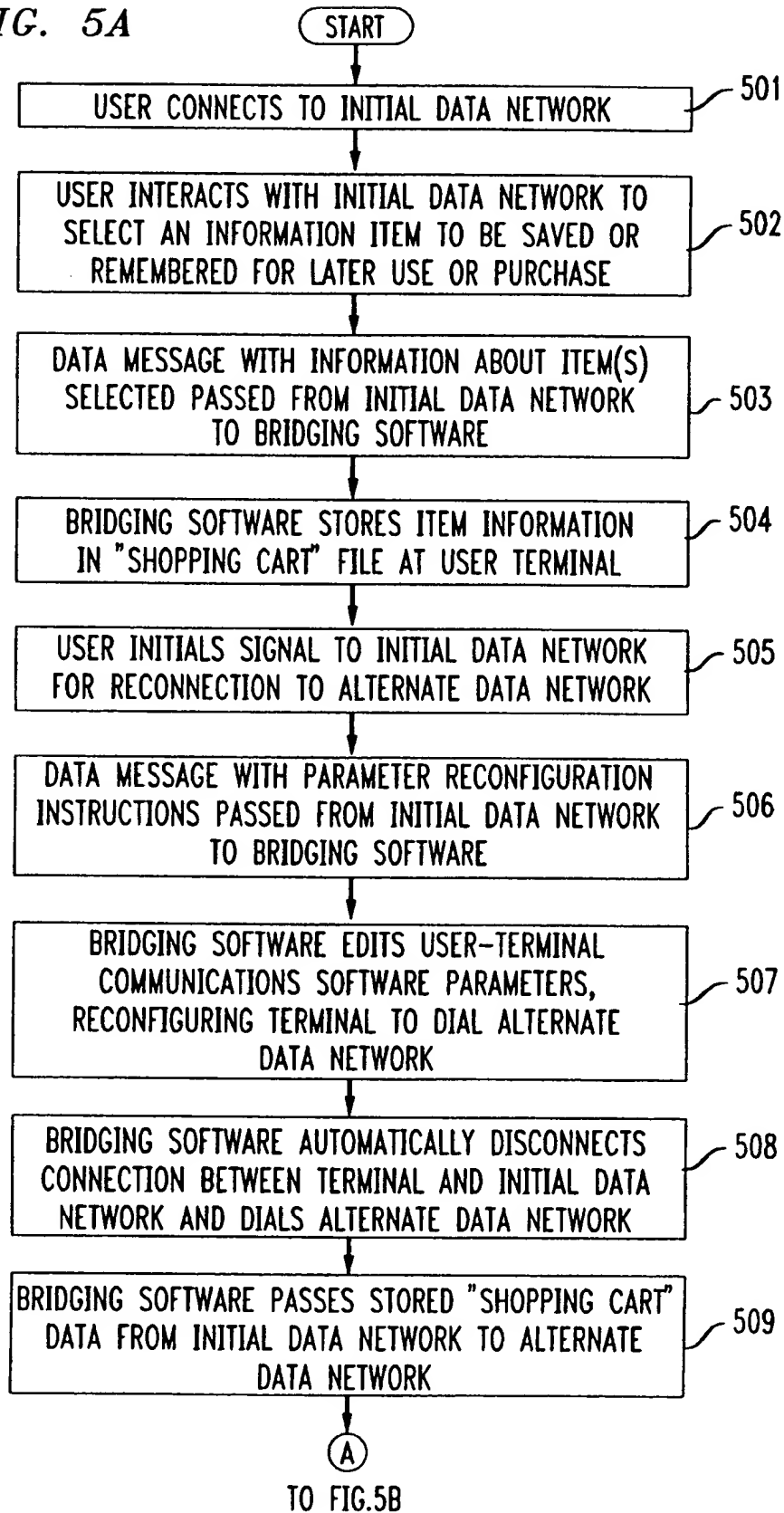


FIG. 5B

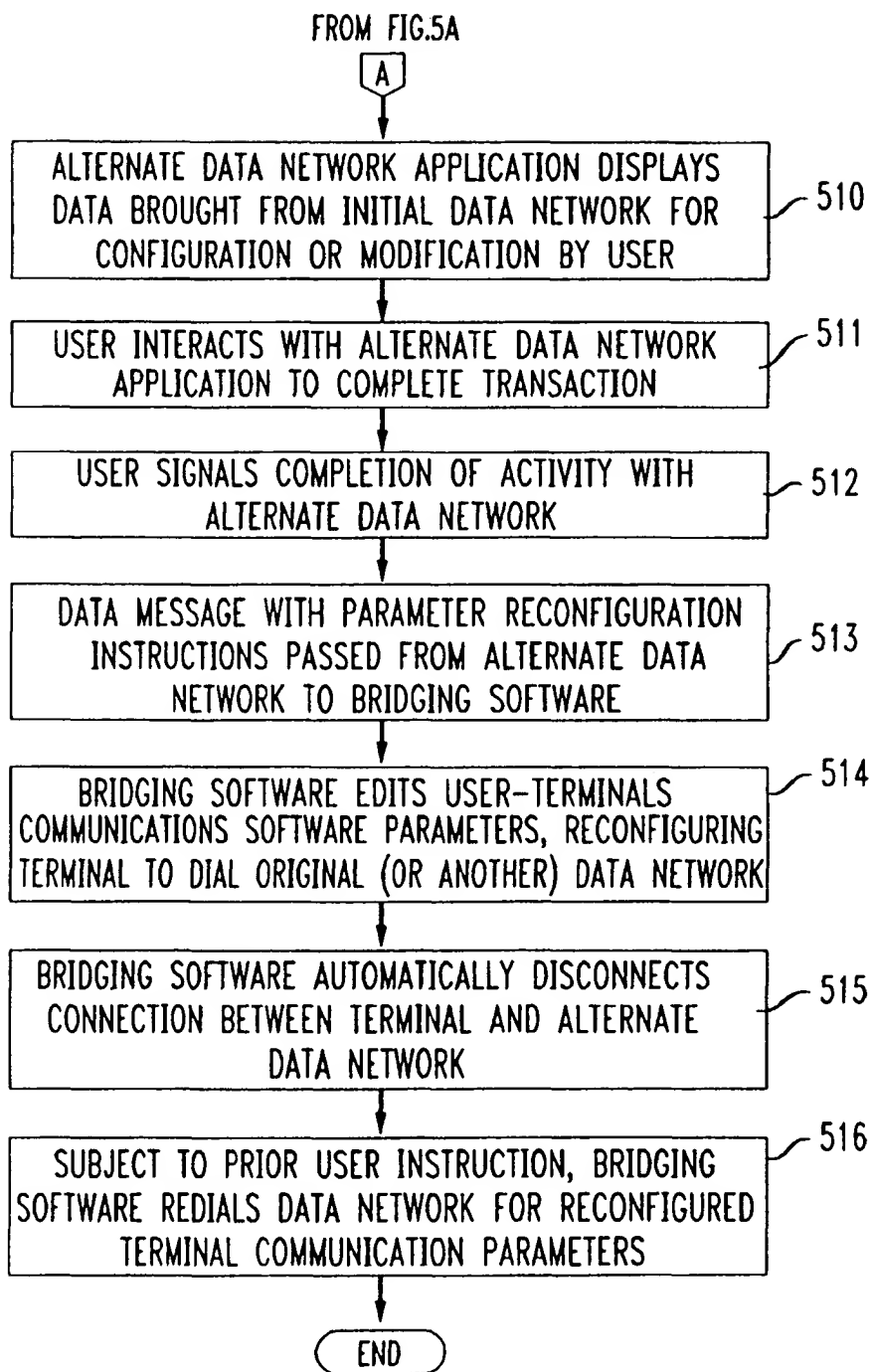


FIG. 6A

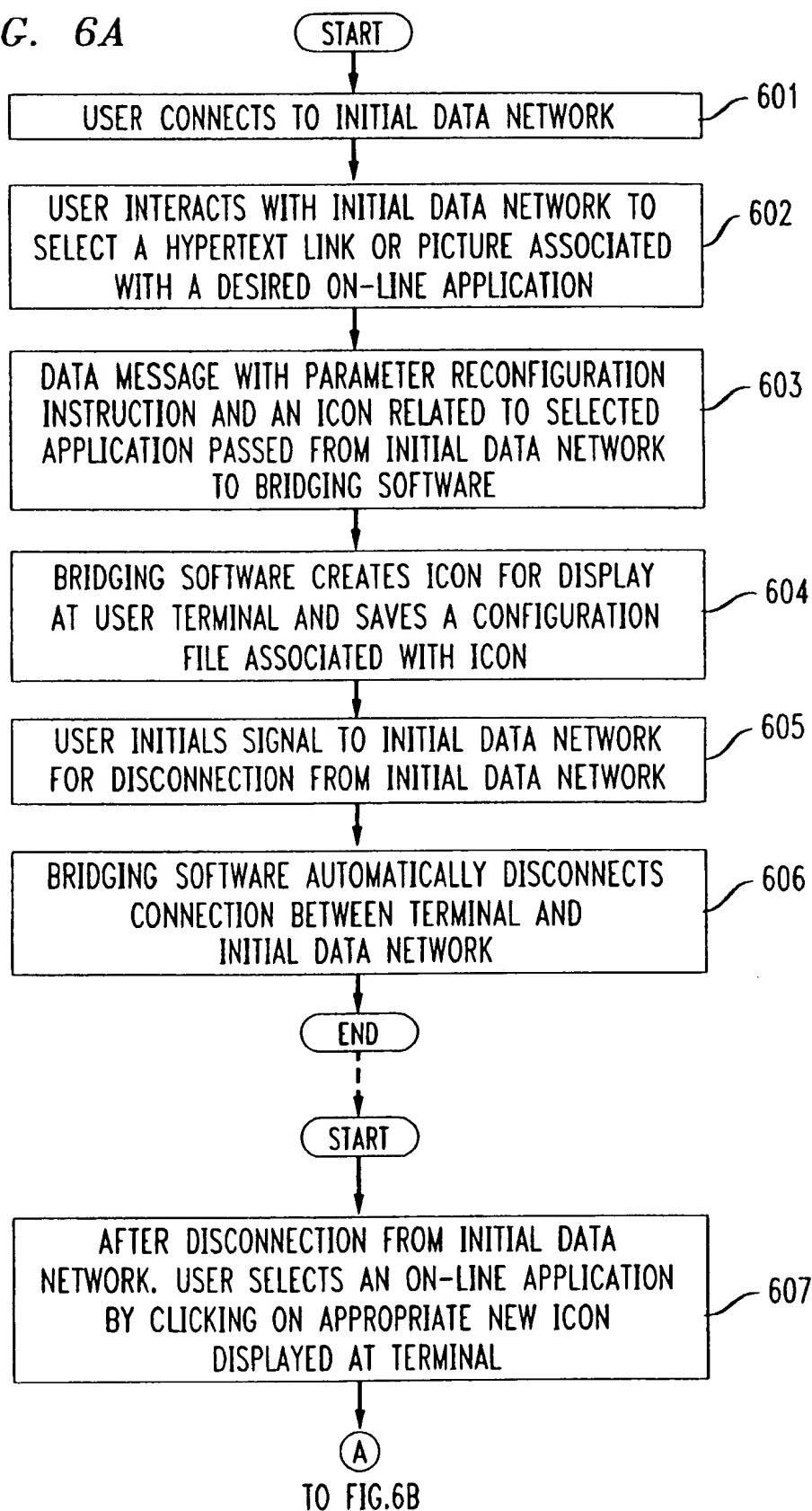




FIG. 6B

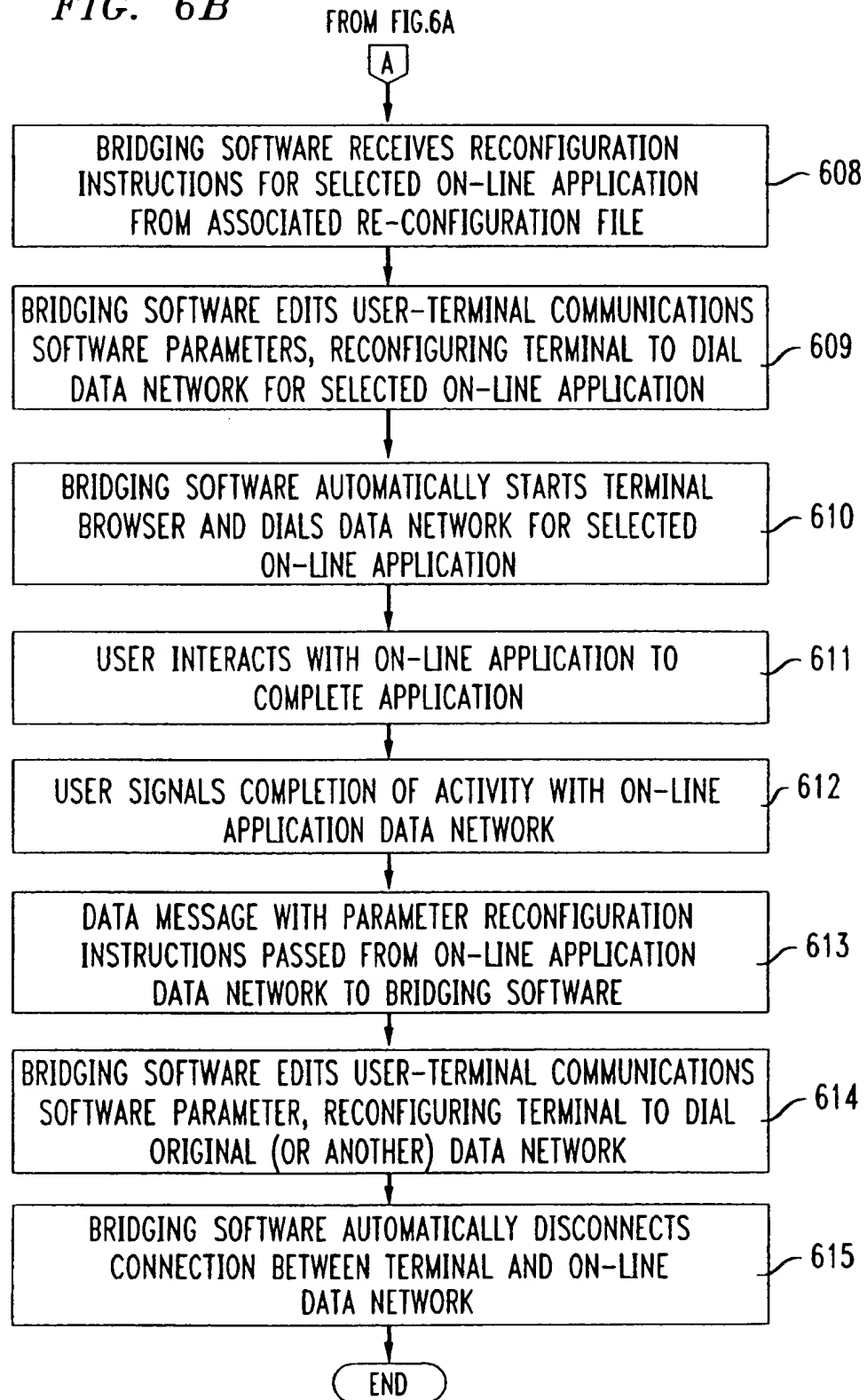


FIG. 7A

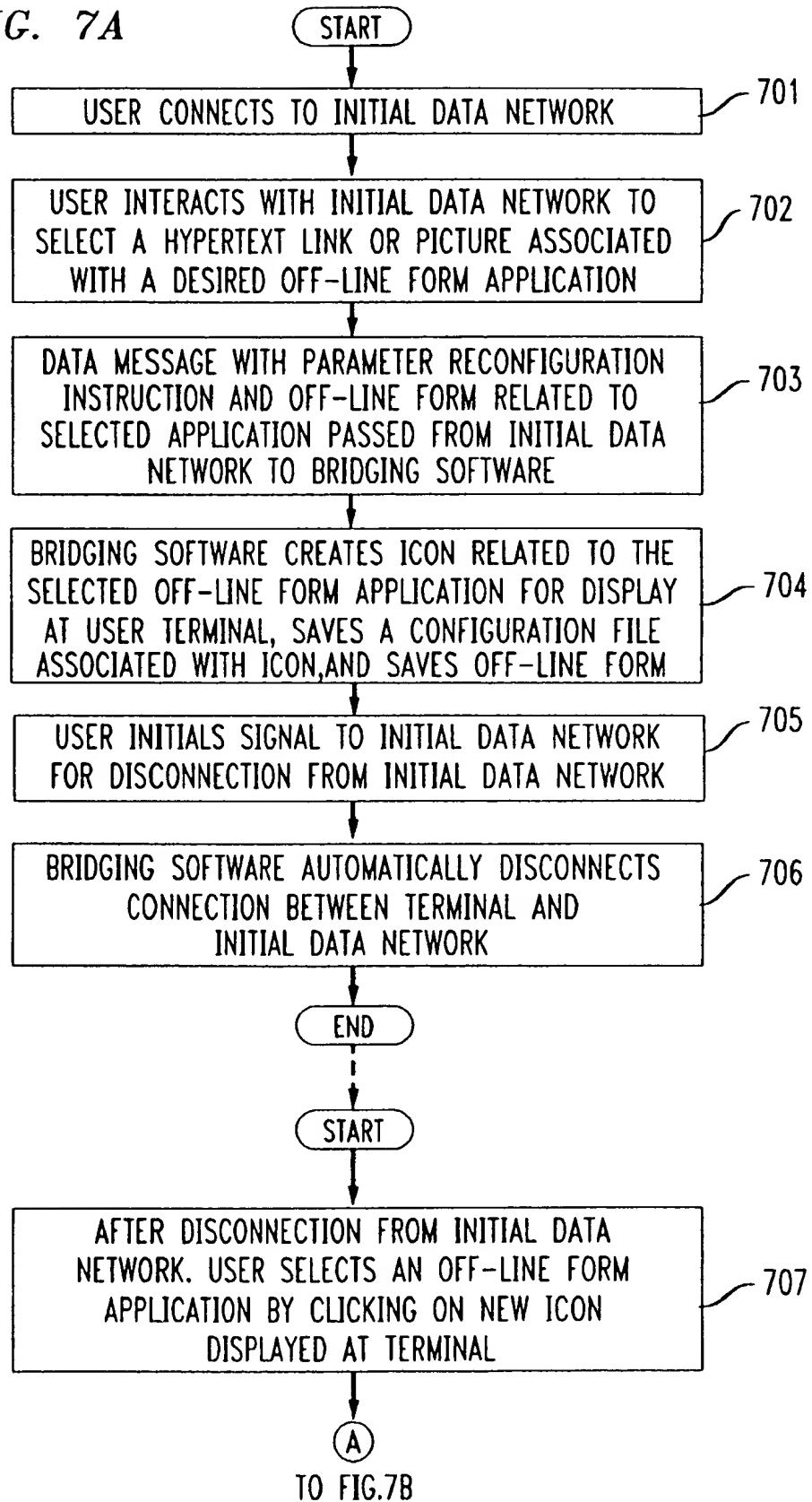
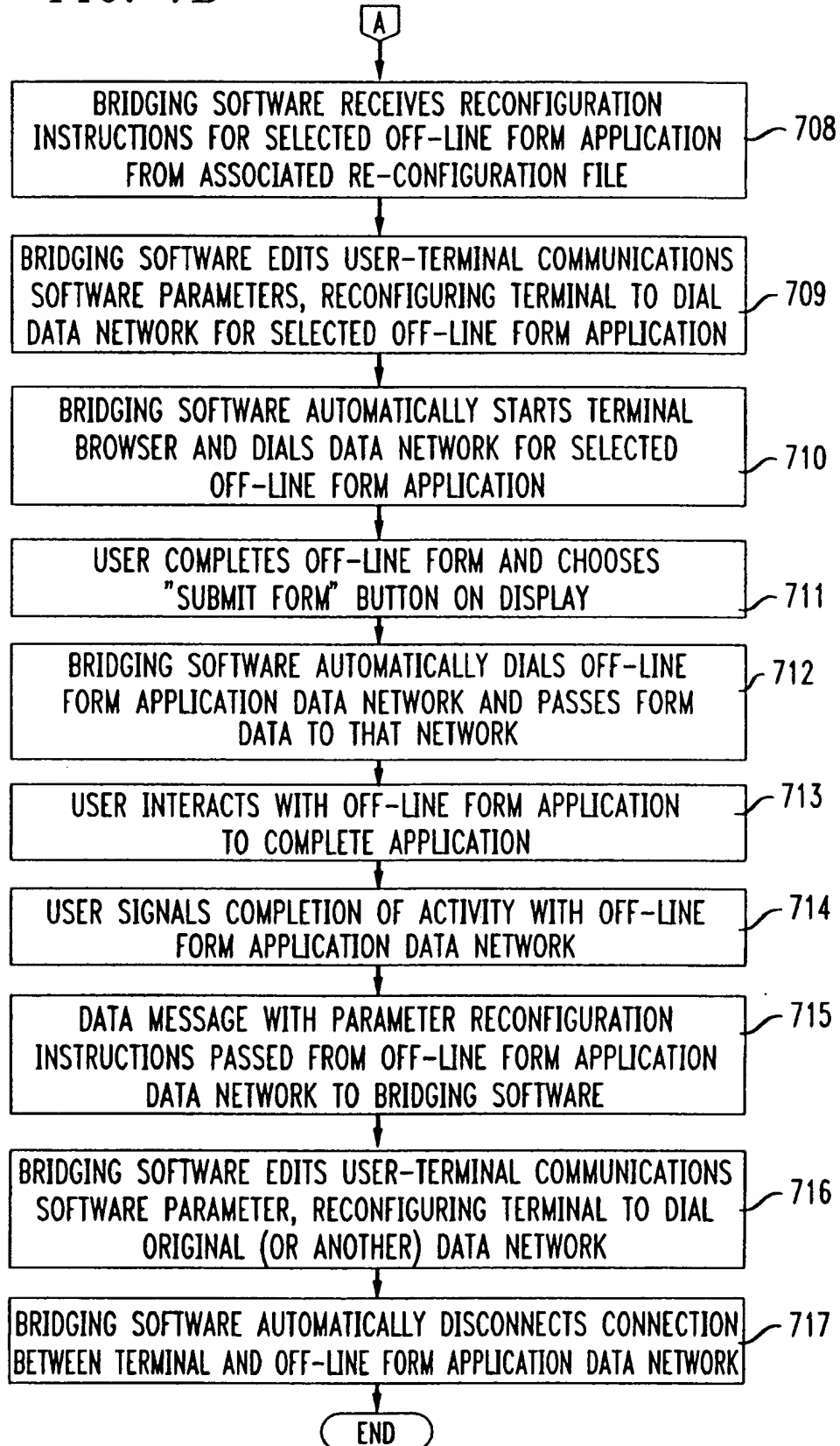
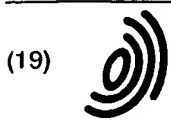


FIG. 7B

FROM FIG.7A





Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) **EP 0 814 589 A3**

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:  
30.08.2000 Bulletin 2000/35

(51) Int. Cl.<sup>7</sup>: **H04L 29/06**, G06F 17/60,  
G07F 19/00

(43) Date of publication A2:  
29.12.1997 Bulletin 1997/52

(21) Application number: **97109792.8**

(22) Date of filing: **16.06.1997**

(84) Designated Contracting States:  
**AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL  
PT SE**

(30) Priority: **19.06.1996 US 667524**

(71) Applicant: **AT&T Corp.**  
**New York, NY 10013-2412 (US)**

(72) Inventors:  
• **Harwood, Jonathan P.**  
**Morganville, N.J. 07751 (US)**

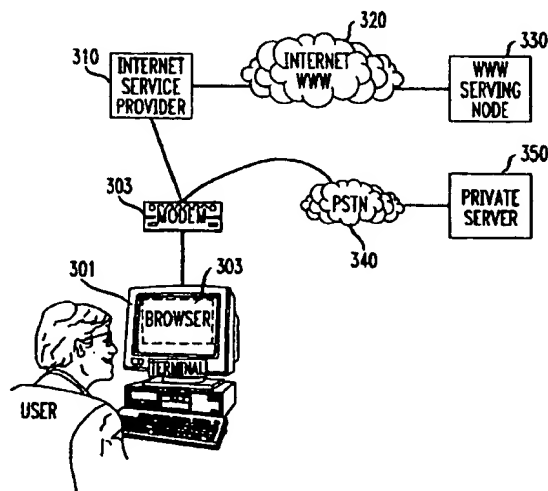
• **Kimmeth, Thomas**  
**Gladstone, N.J. 07977 (US)**  
• **Nusbaum, Kurt**  
**Downers Grove, Illinois 60515 (US)**

(74) Representative: **Kuhnen & Wacker**  
**Patentanwalts-gesellschaft mbH,**  
**Alois-Steinecker-Strasse 22**  
**85354 Freising (DE)**

(54) **System and method for automated network reconfiguration**

(57) A method is disclosed for providing an enhanced level of security for sensitive or proprietary information associated with information transactions in a public network, such as the Internet (101). In carrying out that method, an on-line information transaction is bifurcated between a generalized information access portion of such a transaction and an exchange of sensitive user information. With such a bifurcation, the generalized information access portion of the transaction, which generally would constitute the more substantial (in terms of network resources) portion of the transaction, would be handled via a non-secure network, usually a public network such as the Internet (320). The portion of the transaction involving sensitive user information, on the other hand, would be handled by a separate secure connection, such as a private network, or intranetwork (340). An important characteristic of this bifurcation arrangement is the provision of a means for automated reconfiguration of a user terminal as between accessing the Ageneralized information via the non-secure network and access to the secure communications network for the exchange of sensitive user information. Such an automated reconfiguration will be carried out without the necessity for any action on the part of the user, and indeed will be largely invisible to the user.

**FIG. 3**



**EP 0 814 589 A3**



European Patent  
Office

# EUROPEAN SEARCH REPORT

Application Number  
EP 97 10 9792

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.8)
A	EP 0 590 861 A (AMERICAN TELEPHONE & TELEGRAPH) 6 April 1994 (1994-04-06) * column 1, line 9 - line 24 * * column 3, line 15 - line 17 * * column 3, line 43 - column 4, line 7 *	1-30	H04L29/06 G06F17/60 G07F19/00
A	BAGSHAW E: "NET PROFITS" APRIL 1995 PC PRO, pages 176,178-182, XP002059701 ISSN: 1355-4603 * left-hand column, line 181, last paragraph *	1-30	
A	BELLARE M ET AL: "IKP - A FAMILY OF SECURE ELECTRONIC PAYMENT PROTOCOLS" PROCEEDINGS OF THE FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE, JULY 11-12, 1995, pages 89-106, XP000579445 * page 95, right-hand column *	1-30	
A	WO 96 00485 A (TELEFON AB LM ERICSSON) 4 January 1996 (1996-01-04) * page 6, line 1 - line 3; figure 1 * * page 10, line 13 - page 11, line 29 *	1-30	TECHNICAL FIELDS SEARCHED (Int.Cl.8) H04L G06F G07F
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 5 July 2000	Examiner Vercauteren, S
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons &amp; : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03/82 (Pct/C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT  
ON EUROPEAN PATENT APPLICATION NO.**

EP 97 10 9792

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on  
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-07-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0590861 A	06-04-1994	CA 2100134 A	30-03-1994
		JP 7129671 A	19-05-1995
		MX 9305830 A	30-06-1994
		US 5485510 A	16-01-1996
WO 9600485 A	04-01-1996	US 5668876 A	16-09-1997
		AU 692881 B	18-06-1998
		AU 2688795 A	19-01-1996
		CA 2193819 A	04-01-1996
		EP 0766902 A	09-04-1997
		FI 965161 A	13-02-1997
		JP 10502195 T	24-02-1998

EPD FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

FIG. 1 (Prior Art)

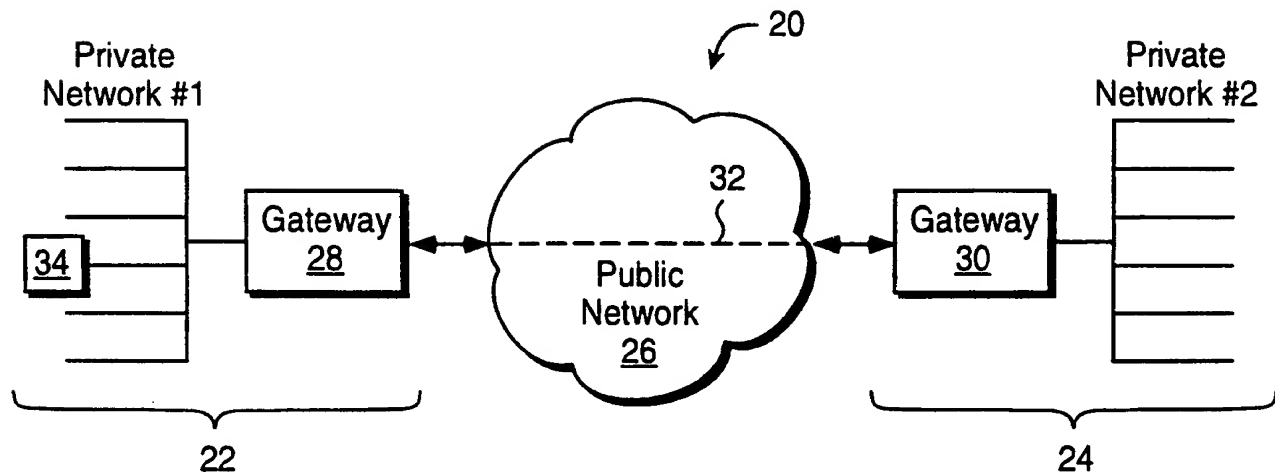


FIG. 2

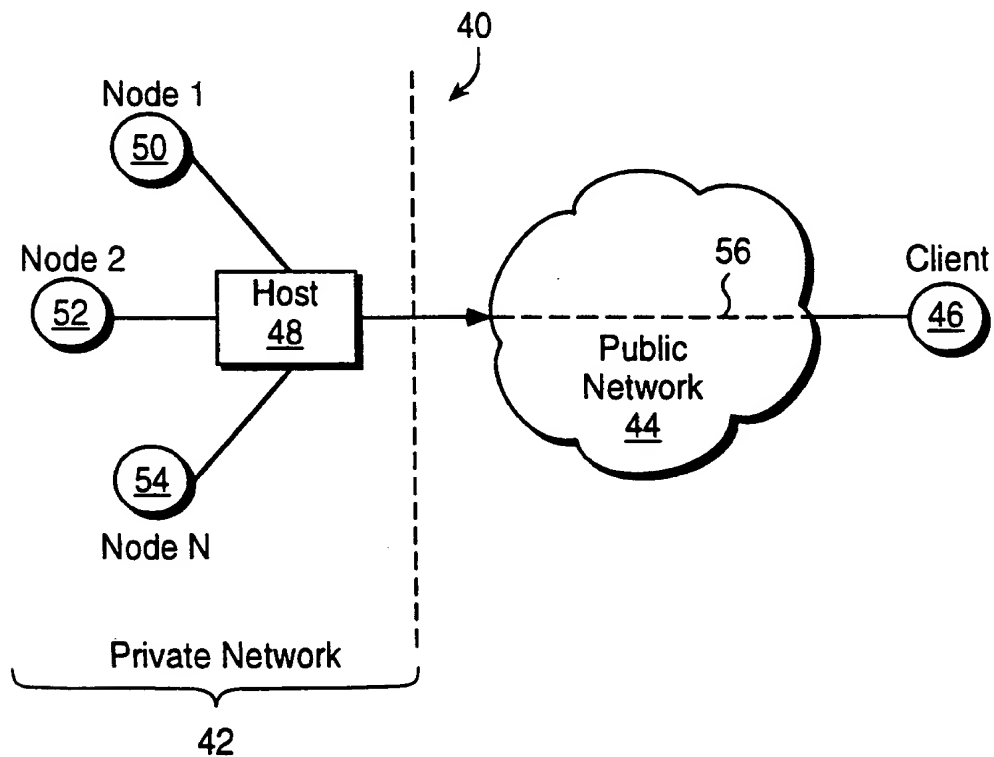
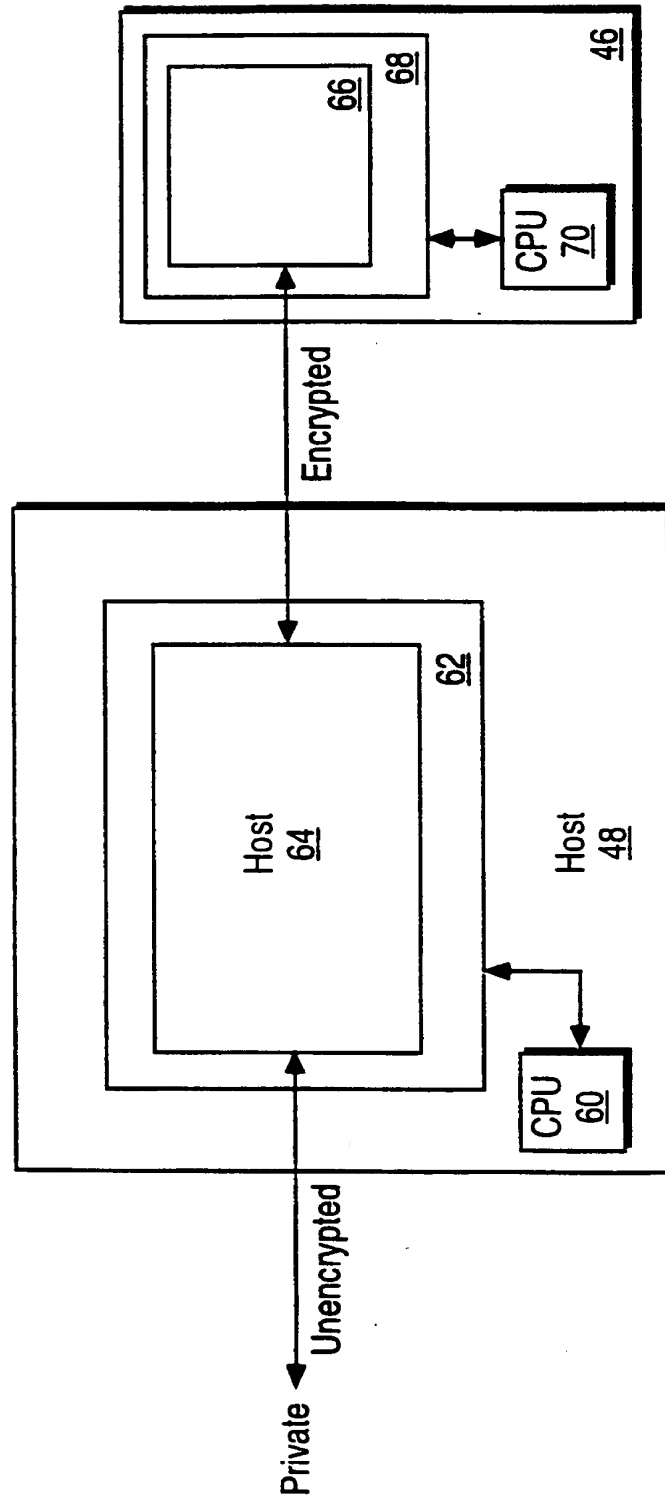


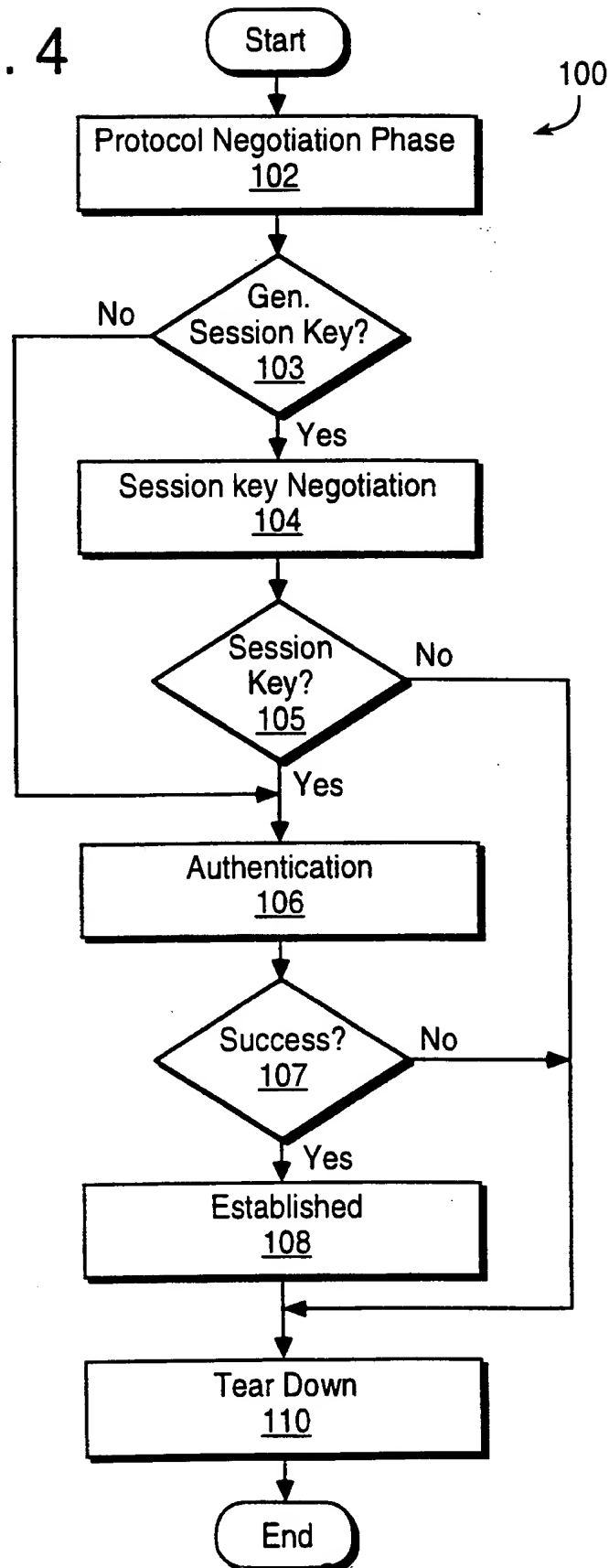
FIG. 3





3/3

FIG. 4



SUBSTITUTE SHEET (RULE 26)

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US99/01583

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 13/00; H04L 9/30

US CL : 709/245 . 229 : 380/30

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/245 . 229, 228, 226: 380/30 . 23

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, Internet

Search terms : private and public network, protocols, authentication, session key, encrypt, decrypt, encapsulation.

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,416,842 A (AZIZ) 16 MAY 1995, Abstract, Figs. 2 and 5 and 6, col. 4 line 65 - col. 5 line 48, col. 6 lines 3-35 and lines 40-51, col. 7 lines 16-35, col. 7 line 63 - col. 8 line 2	1-14
Y	US 5,550,984 A (GELB) 27 AUGUST 1996, Abstract, Fig. 1, col. 5 line 45 - col. 6 line 51, col. 7 line 58 - col. 8 line 19	1-14
Y	US 5,548,646 A (AZIZ ET. AL.) 20 AUGUST 1996, Abstract, Figs. 5 and 6, col. 9 lines 1-50, col. 10 line 32 - col. 11 line 67	1-14
Y,P	US 5,835,726 A (SHWED ET. AL.) 10 November 1998, Abstract, Fig. 21, col. 20 line 41 - col. 21 line 7, col. 22 line 19 - col. 23 line 9.	1-14



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents.	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
*A* document defining the general state of the art which is not considered to be of particular relevance	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
*E* earlier document published on or after the international filing date	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Z* document member of the same patent family
*O* document referring to an oral disclosure, use, exhibition or other means	
*P* document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

21 MAY 1999

Date of mailing of the international search report

02 JUN 1999

Name and mailing address of the ISA/US  
Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

AHMAD MATAR

Telephone No. (703) 305-4731